REMARKS:

In the outstanding Office Action, claims 1-15 were rejected. New claim 16 has been added. No new matter has been added. Thus, claims 1-16 are pending and under consideration. The outstanding rejections are traversed below.

REJECTION UNDER 35 U.S.C. §103(a):

In the outstanding Office Action, claims 1-4, 6-11 and 13-15 were rejected under 35 U.S.C. §103(a) as being unpatentable over Recent Developments in the Design of Conventional Cryptographic Algorithms reference by Preneel et al. ("Preneel") in view of U.S. Patent No. 6,501,840 ('840). Claims 5 and 12 were rejected under 35 U.S.C. §103(a) as being unpatentable over Preneel, in view of '840 and further in view of U.S. Patent No. 6,182,216 ('216).

Preneel discusses a cryptographic method using S-boxes for nonlinear functions where the important concern is that the S-boxes fit in a fast cache memory.

'840 discusses a cryptographic processing method where an input data size is calculated based on message to be sent so that a design of a user apparatus does not need to be changed when a new cryptographic processing type or a new algorithm type is used.

'216 discusses a block cipher method for encrypting a preset 128-bit or more input block where the input block is divided into 2 or 4 data segments.

The present invention discloses a cipher logic design method and apparatus where an input bit size and an output bit size of each S-box is determined based on a memory capacity in the cipher device.

The Examiner compares the Preneel reference discussing the use of S-boxes where 8 input bits are transformed into 32 or 64 output bits to the present invention where input and output bits of S-boxes is determined based on a memory capacity of the cipher device. In Preneel, S-boxes are discussed where 8 input bits are transformed into 32 or 64 output bits (see, page 113, paragraph 3 in section 4.2 of Preneel). The Preneel reference further discusses examples of ciphers using 8 → 32 S-boxes, such as Blowfish, Khufu, CAST, and SQUARE, and examples of ciphers using 8 → 64 S-boxes, such as SHARK and SQUARE (see, page 113, paragraph 3 in section 4.2 of Preneel). The Preneel reference teaches that S-boxes with 8 input bits and 32 or 64 output bits provide higher efficiency and are particularly suited for 32-bit or 64-bit processors (see, page 118, lines 1-10 of Preneel). The discussion in relation to S-boxes in the Preneel reference is limited to S-boxes with 8 input bits where output bits are

expanded to 32-bits or 64-bits. This means that Preneel is directed to extending output bits based on fast cache memory.

The Examiner acknowledges that Preneel does not explicitly disclose selecting an input and output bit number of the S-boxes and generating the S-boxes where each has the input and output number selected, thus relies on '840 as providing the same. In the '840 system, an input unit (122) receives inputs of a cryptographic processing type, an algorithm type, and contents of a message to be sent using the cryptographic processing type (see, column 5, lines 22-27 of '840). Then, an input data size calculation unit (127) calculates input data size of cipher text or plain text transferred from a cryptographic processing unit (115), and outputs the calculated input data size to an output data size judgement unit (114) (see, column 5, lines 51-55 of '840). The output data size judgement unit (114) calculates an output data size based on the received input data size, and outputs the calculated output size (see, column 6, lines 42-46 of '840). This means that in the '840 system, input and output data is not optimized for each block because the input data size, upon which the output data size depends, is extracted from input data/message to be sent.

A cipher designing apparatus and method of the present invention designs cipher logic per block using an F-function for converting input bits to output bits via a plurality of S-boxes. As recited in independent claims 1, 8 and 15, the cipher designing apparatus and method includes "selecting an input and output bit number of said plurality of S-boxes based on a memory capacity of a high-speed referable memory provided to said cipher device". Unlike the discussion in Preneel where input bits are limited to 8 bits and unlike the '840 system where input bits are determined based on input data to be sent, the present invention selects an input and output bit number of the S-boxes "based on a memory capacity of a high-speed referable memory provided to said cipher device". For example, for a 32-bit nonlinear transformation where the processor includes a memory having 32 Kbytes, the 32 input bits are divided into 11, 10, 11 where only three S-boxes are used (see, FIG. 2 and corresponding text of the present application). In contrast, the 32-bit nonlinear transformation according to Preneel will be divided into 8, 8, 8, 8 where four S-boxes would need to be used. Accordingly, processing speed is increased by as much as 25% according to the cipher logic design method of the present invention in comparison to Preneel.

Moreover, the cipher designing apparatus and method includes an S-box generating unit that "generates a plurality of S-boxes each having the input and output bit number selected by said selecting unit" (see, independent claims 1, 8 and 15 of the present invention). This allows the reduction of the number of times the S-boxes need to be accessed and thus, realizes high-

speed cipher/decryption of data.

The combination of the Preneel reference and the '840 system leads to a cryptographic method using S-boxes for nonlinear functions where a preset input data size is used, and where the input data size is calculated based on message to be sent.

It is respectfully submitted that independent claims 1, 8 and 15 reciting a cipher logic design method and apparatus where input and output bit numbers of S-boxes are selected "based on a memory capacity of a high-speed referable memory provided to said cipher device" are patentably distinguishable over the combination of Preneel and '840.

For at least the above-mentioned reason, dependent claims depending from independent claims 1, 8 and 15 are patentably distinguishable over the combination of the cited references. For example, as recited in claims 5 and 12, the cipher designing method of the present invention includes "specifying a smallest value of the input and output number of said plurality of S-boxes". The Examiner acknowledges that Preneel as modified does not disclose the features recited in claims 5 and 12, thus relies on '216 as disclosing the same. The '216 system is directed to a method for encrypting a predetermined 128-bit or more input block where the input block is divided into data segments (see, column 16, lines 55-65 of '216).

The combination of Preneel, '840 and '216 leads to a cryptographic method using S-boxes where the S-boxes are used for nonlinear functions and have preset input data size, and where the input data size is calculated based on message to be sent and is preferably 128-bit. This does not teach or suggest "selecting an input and output bit number of said plurality of S-boxes based on a memory capacity of a high-speed referable memory provided to said cipher device", and "generating a plurality of S-boxes each having the input and output bit number selected by said selecting unit" as recited in independent claims 1 and 8, from which claims 5 and 12 depend, respectively.

The burden of establishing a prima facie case of obviousness based upon the prior art lies with the Examiner. In re Fritch, 23 U.S.P.Q. 2d 1780, 1783 (Fed. Cir. 1992). According to In re Fritch, the Examiner "... can satisfy this burden only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references." The combination of Preneel, '840 and '216 does not teach or suggest selection of input and output bits of S-boxes based on a memory capacity of a memory provided to the cipher device".

It is respectfully submitted that the Examiner has not met the burden of establishing a prima facie case of obviousness. Thus, withdrawal of the rejection is respectfully requested.